

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

Launching of (electro)mechanical process with user identification from file

Patent number: FR2760874
Publication date: 1998-09-18
Inventor: FRUNEAU PATRICK
Applicant: FDI MATELEC SA (FR)
Classification:
- **International:** G07C1/00; G07C9/00; E05B49/00
- **European:** G07C9/00C2B
Application number: FR19970002972 19970311
Priority number(s): FR19970002972 19970311

Abstract of FR2760874

The control of authorisation to launch a process is based on electronic keys co-operating with a file of forbidden electronic keys. The electronic key holds all the information necessary for the launching of the process. The electronic keys are encoded using a code word linked to a particular process management group. Each key authorisation can decode the key information and determine its originating group. Each key carries a number of passwords to selection of an authorised process. The authorisation centres have a password to permit selection of the electronic key and authorise it to launch the process. Forbidden keys are identified from a file.

①⑨ RÉPUBLIQUE FRANÇAISE
INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE
PARIS

①⑪ N° de publication : **2 760 874**
(à n'utiliser que pour les
commandes de reproduction)
②① N° d'enregistrement national : **97 02972**

⑤① Int Cl⁶ : G 07 C 1/00, G 07 C 9/00, E 05 B 49/00

①⑫ **DEMANDE DE BREVET D'INVENTION** **A1**

②② Date de dépôt : 11.03.97.

③⑩ Priorité :

④③ Date de mise à la disposition du public de la
demande : 18.09.98 Bulletin 98/38.

⑤⑥ Liste des documents cités dans le rapport de
recherche préliminaire : *Ce dernier n'a pas été
établi à la date de publication de la demande.*

⑥⑩ Références à d'autres documents nationaux
apparentés :

⑦① Demandeur(s) : *FDI MATELEC SA SOCIETE ANO-
NYME — FR.*

⑦② Inventeur(s) : FRUNEAU PATRICK.

⑦③ Titulaire(s) :

⑦④ Mandataire(s) :

⑤④ NOUCEN.

⑤⑦ Dispositif de lancement de processus dont la vérifi-
cation de l'identité du demandeur est basée sur la gestion d'un
fichier des demandeurs interdits.

L'invention est constituée de clefs électroniques servant
à identifier le demandeur de lancement de processus, de
lecteurs de clefs électroniques servant à sélectionner le pro-
cessus à lancer, de centrales d'autorisations servant de
centre de décision, et de programmeurs de clefs électro-
niques servant à exploitation du système par le gestionnai-
re.

Le dispositif selon l'invention est particulièrement desti-
né aux systèmes de lancement de processus dont la vérifi-
cation de l'identité et des niveaux d'autorisations des
demandeurs sont nécessaires.

FR 2 760 874 - A1



DESCRIPTION GENERALE

10 La présente invention concerne un système de lancement de processus dont la vérification de l'identité du demandeur est basée sur la gestion d'un fichier des demandeurs interdits.

15 L'invention est destinée à toute application de lancement de processus ayant besoin de l'identification du demandeur avant le lancement dudit processus. A titres d'exemples, l'invention s'applique à la commande de processus automatique ou semi-automatique, mécanique ou électromécanique, comme la commande d'un moteur, d'une électrovanne, d'un électro-aimant, d'une
20 serrure ou tout autre système.

 Les méthodes mécaniques actuellement utilisées pour le lancement de processus font appel à des clefs mécaniques. Ces clefs, qui par l'intermédiaire d'une serrure, actionnent soit
25 des cames, soit des vannes, soit des interrupteurs électriques ou autres, assurent le lancement du processus.

 En cas de perte, ou de vol, la gestion par clefs mécaniques met en oeuvre toute une structure qui va de la personne fautive
30 au serrurier. Dans le cas le plus simple, la personne fautive doit en faire par à son gestionnaire qui doit en faire par au serrurier. Lequel serrurier doit changer toutes les serrures acceptant cette clef perdue ou volée et revoir la hiérarchie des clefs dans le cas où la même clef permet le lancement de
35 plusieurs processus. Une fois cela fait, le gestionnaire doit contacter et changer les clefs de toutes les personnes ayant droit au lancement des mêmes processus que ceux autorisés par la clef perdue ou volée.

40 De même il existe actuellement des méthodes électroniques utilisées pour le lancement de processus faisant appel à des

2

5 clefs électroniques. Ces clefs, qui par l'intermédiaire d'une serrure électronique, actionnent soit des relais, soit des électrovannes, soit des transistors ou autres, assurent le lancement du processus.

10 Comme pour les clefs mécaniques, en cas de perte ou de vol, il faut que la personne fautive avertisse son gestionnaire. Cette personne gérant le système doit passer sur chacune des serrures électroniques pour invalider la clef électronique perdue ou volée, puis programmer une nouvelle clef électronique
15 et la valider sur chacune des serrures électroniques. En cas de perte ou de vol du programmeur de clefs électroniques, le système n'est plus sécurisé car la duplication et la création de clef électronique sont aisément possible.

20 Il faut noter que la duplication de clef électronique demande une mise en oeuvre plus complexe que son homologue mécanique mais est possible. Pour éviter au gestionnaire le déplacement sur toutes les serrures électroniques, celles-ci sont reliées par un réseau local dédié ce qui permet une gestion
25 centralisée.

Que les systèmes soient mécaniques ou électroniques, en cas de malveillance ou de vandalisme, on peut lancer le processus de façon relativement aisé. En démontant ou cassant le carter de la
30 serrure mécanique ou électronique on a accès aux éléments mécaniques ou électromécaniques qui lancent le processus.

Un autre problème sur les systèmes mécaniques ou électroniques est que les fabricants et les installateurs du
35 matériel qui, pour leurs tests possèdent des clefs donnant accès au lancement de processus.

Sur les systèmes électroniques, la programmation des clefs électroniques se fait par un programmeur qui demande
40 l'intermédiaire d'un ordinateur ou d'un terminal pour pouvoir être opérationnel. De même des serrures électroniques demandent

3

5 l'intermédiaire d'un ordinateur ou d'un terminal pour leur utilisation et programmation. Ce matériel nécessaire à l'exploitation du système est lourd, coûteux et d'une utilisation complexe.

10 On voit que ces systèmes, mécaniques ou électroniques demandent une installation, une gestion et une maintenance contraignante.

L'invention qui résout les contraintes et les inconvénients
15 de ces systèmes a une architecture basée sur les éléments suivants: les clefs électroniques, les lecteurs de clefs électroniques, les centrales d'autorisations et les programmeurs de clefs électroniques.

Selon l'invention basée sur l'organisation de la gestion
20 d'un fichier des interdits il n'est pas nécessaire de programmer et de maintenir à jour un fichier des clefs électroniques autorisées à lancer les processus.

Pour éviter d'avoir accès au lancement du processus en cas
25 de démontage ou de vandalisme sur les lecteurs de clefs électroniques, ceux-ci ne possèdent pas d'éléments permettant le lancement direct du processus. Seules les centrales d'autorisations possèdent le moyen de lancer des processus. Les lecteurs de clefs électroniques ont uniquement pour fonction la
30 vérification de la cohérence du contenu des clefs électroniques et la liaison avec les centrales d'autorisations. La liaison entre la serrure électronique et la centrale d'autorisation se fait de façon encodée pour éviter le piratage de la ligne. La liaison avec les centrales d'autorisations se fait sur 2 fils
35 servant à la fois de ligne d'alimentation des lecteurs de clef électronique et de ligne de communication avec les centrales d'autorisations.

Dans le cas de clef électronique à contacts, le lecteur de
clef électronique est remplacé par un système de contact
40 uniquement mécanique. Cela accroît la sécurité du système car le démontage du lecteur de clef électronique ne donne pas d'accès à

4

5 l'électronique du système. Avec ce lecteur de clefs
électroniques uniquement mécanique, la centrale d'autorisation
se substitue au lecteur de clef électronique et effectue elle-
même la vérification de la cohérence du contenu des clefs
électroniques.

10

Pour éviter une installation demandant la réalisation d'un
réseau local, les clefs électroniques permettent le stockage de
toutes les informations relatives à leurs autorisations de
lancement de processus. Grâce aux informations contenues dans
15 les clefs électroniques, les centrales d'autorisations peuvent
interdire ou autoriser le lancement de processus sans avoir
besoin d'un fichier des clefs électroniques en service. Ces
informations seront désignées par le vocabulaire, passe,
autorisation d'accès, identification, exemplaire, groupe
20 horaire, début de validité, fin de validité et caractères de
contrôles. L'explication de ce vocabulaire se fera au fur et à
mesure de la description du système. Ces informations de gestion
sont enregistrées dans les clefs électroniques par le
gestionnaire au moment de leur programmation ce qui permet une
25 gestion centralisée. Les centrales d'autorisation n'ayant pas de
fichier à programmer, cela évite l'installation d'un réseau pour
avoir une gestion centralisée et garder leurs fichiers à jour.

Pour éviter qu'un gestionnaire puisse avoir accès à d'autres
30 processus que ceux placés sous sa gestion, le système fait appel
à des mots d'encodages déterminés par le gestionnaire. Les clefs
électroniques seront encodées à l'aide de ce mot d'encodage
déterminé par le gestionnaire. Seules les centrales
d'autorisations programmées pour reconnaître ce mot d'encodage
35 pourront accepter les clefs électroniques ayant été encodées par
ce même mot d'encodage et autoriser le lancement du processus
demandé. Ce mot d'encodage propre au gestionnaire interdit les
clefs électroniques créées par le fabricant ou l'installateur
au moment des tests. De même les clefs électroniques créées par
40 un autre gestionnaire seront interdites.

5

5 Pour éviter qu'un cas de perte ou de vol du programmeur de
clef il soit possible de créer des clefs électroniques, celui-ci
ne possède ni ne mémorise le mot d'encodage. Le mot d'encodage
devra être saisi sur le programmeur par le gestionnaire avant
la programmation des clefs électroniques.

10

Pour éviter d'avoir à demander l'intermédiaire d'un
ordinateur ou d'un terminal pour programmer les clefs
électroniques et programmer les centrales d'autorisations, on
utilise un petit terminal portable alimenté par batterie. Ce
15 terminal portable possède, un clavier alphanumérique, un écran,
un lecteur/programmeur de clefs électronique et une liaison
sans fil (infrarouge ou radiofréquence). En mode autonome, le
terminal portable permet la programmation des clefs
électroniques. Par contre pour programmer les centrales
20 d'autorisations, les écrans et les informations de gestions sont
transmis par les centrales d'autorisations à travers la liaison
sans fil. Le fait que le terminal portable ne possède pas les
écrans et les informations de gestions des centrales
d'autorisations permet de limiter la taille, l'encombrement et
25 augmenter le temps d'autonomie du terminal portable.

Pour sélectionner les processus pouvant être lancés par les
clefs électroniques avec des centrales d'autorisations n'ayant
pas de fichier, on utilise les notions de passe et
30 d'autorisation d'accès. La notion de passe permet une sélection
au niveau des centrales d'autorisations. La notion
d'autorisation d'accès permet une sélection au niveau des
processus car les centrales d'autorisations peuvent gérer
plusieurs processus. A chaque processus contrôlé par une
35 centrale d'autorisation, correspond un lecteur de clefs
électroniques et un numéro d'autorisation d'accès. Les clefs
électroniques possèdent une zone de données réservée à un numéro
de passe et une zone de données réservée aux numéros
d'autorisations d'accès. Les centrales d'autorisations possèdent
40 une zone de données réservée aux numéros de passe et une zone de
données réservée aux numéros d'autorisations d'accès. Les

6

5 centrales d'autorisations qui mémorisent plusieurs numéros de
passes permettent à une clef électronique de pouvoir lancer des
processus distribués sur plusieurs centrales d'autorisations.
Les clefs électroniques mémorisent plusieurs numéros
d'autorisation d'accès pour pouvoir lancer plusieurs processus.
10 Pour qu'un processus soit lancé il faut que le numéro
d'autorisation d'accès du processus corresponde à un des numéros
d'autorisations d'accès de la clef électronique.

Pour éviter d'avoir à programmer toutes les clefs
15 électroniques autorisées dans toutes les centrales
d'autorisations, celles-ci font uniquement une gestion des clefs
électroniques interdites avec la notion d'identification et
d'exemplaire. Les clefs électroniques possèdent une zone de
données réservée à un numéro d'identification et à un numéro
20 d'exemplaire. Pour toutes les clefs électroniques qui effectuent
une demande de lancement de processus, la centrale
d'autorisation vérifie que le numéro d'identification et le
numéro d'exemplaire de la clef électronique n'est pas présent
dans son fichier des clefs électroniques interdites. Si le
25 numéro d'identification et le numéro d'exemplaire de la clef
électronique sont présents dans le fichier des clefs
électroniques interdites, la demande de lancement de processus
sera refusée.

30 Pour éviter au gestionnaire un déplacement sur les sites,
dans le cas de perte ou de vol des clefs électroniques, la
centrale d'autorisation effectue une mise à jour automatique de
son fichier des clefs électroniques interdites. Pour effectuer
cette mise à jour, les centrales d'autorisation utilisent le
35 numéro d'identification et le numéro d'exemplaire. Lorsqu'une
demande de lancement de processus est effectuée avec une clef
électronique ayant le numéro d'identification i et le numéro
d'exemplaire e supérieur à 1, le numéro d'identification i et le
numéro d'exemplaire $e-1$ sont enregistrés dans le fichier des
40 clefs électroniques interdites. La centrale d'autorisation
interdit alors le lancement de processus par toutes les clefs

7

- 5 électroniques ayant le même numéro d'identification et ayant un
numéro d'exemplaire inférieur ou égal à ceux présent dans son
fichier de clefs électroniques interdites. Lors de leurs
première mise en service, les clefs électroniques sont
programmées avec le numéro d'exemplaire $e = 1$. Pour toutes
10 demandes de lancement de processus effectuées avec une clef
électronique ayant le numéro d'exemplaire $e = 1$, la centrale
d'autorisation ne modifie pas son fichier des clefs
électroniques interdites.
- 15 Pour limiter dans le temps l'autorisation de lancement de
processus, on utilise la notion de début et de fin de validité.
Les clefs électroniques possèdent une zone de données réservée
pour les dates de début et de fin de validité. Les centrales
d'autorisations utilisent ces dates de début et de fin de
20 validité par comparaison avec la date (dans tout le texte on
entend par date les jours du mois, les mois et les années) de
son horloge interne pour autoriser ou interdire le lancement un
processus. La date de début de validité permet de créer et de
distribuer les clefs électroniques aux utilisateurs avant la
25 date donnant droit au lancement de processus. La date de fin de
validité permet d'interdire les clefs électroniques dans le cas
où les utilisateurs ne rendent pas les clefs électroniques au
gestionnaire.
- 30 Pour limiter les horaires d'autorisation de lancement de
processus jour par jour, on utilise la notion de groupe horaire.
Les clefs électroniques possèdent une zone de données réservée à
un numéro de groupe horaire. Les centrales d'autorisation
possèdent une zone de données réservée pour des tables
35 d'horaires. Chaque table d'horaire est associée à un numéro de
groupe horaire. Le numéro de groupe horaire est utilisé par les
centrales d'autorisations pour sélectionner une des tables
donnant les horaires pendant lesquelles une clef électronique a
le droit de lancer un processus. Ces tables d'horaires
40 définissent les horaires d'autorisation de lancement des
processus sur une semaine. Les jours de cette semaine sont

8

5 découpés en tranches donnant les heures et minutes de début et de fin d'autorisation de lancement des processus. Dans le cas de clef électronique disposant de suffisamment de mémoire, la table d'horaire est enregistrée par la clef électronique.

10 Les centrales d'autorisations utilisent cette table d'horaire par comparaison avec l'heure (dans tout le texte on entend par l'heure les heures et les minutes) de son horloge interne pour autoriser ou interdire le lancement un processus.

15 La notion de caractères de contrôle est utilisée pour vérifier la validité et de cohérence des informations de la clef électronique. Cela peut aller du simple LRC à une signature informatique.

20 Certains processus doivent pouvoir être lancés à distance en utilisant des technologies infrarouges ou radiofréquences et d'autre pouvoir être lancés à proximité en utilisant des technologies de proximités ou de contacts. Cette demande est aussi faite pour la rénovation de site où l'on ne peut pas changer les lecteurs de clefs électroniques qui utilisent des
25 moyens différents pour la communication avec les clefs électroniques. Les clefs électroniques peuvent pouvoir regrouper plusieurs technologies différentes pour la communication avec les lecteurs, cela leur permet d'accéder à des processus distants ou proches suivant les cas.

5

DESCRIPTION DES FIGURES

Les éléments selon l'invention des figures 1 et 2 donnent une présentation générale de la structure du système avec les clefs électroniques « CLEL » possédant un numéro de groupe
 10 horaire « GRHO » et des centrales d'autorisation possédant des tables d'horaires « TAHO ».

Les éléments selon l'invention des figures 3 et 4 donnent une présentation générale de la structure du système avec les clefs électroniques « CLEL » possédant une table horaire «
 15 TAHO » et des centrales d'autorisation sans tables d'horaires.

Les éléments selon l'invention des figures 5 et 6 donnent un exemple d'application particulière de l'invention.

Sur la figure 1 on retrouve la clef électronique « CLEL »
 20 encodée par le mot d'encodage « MOEN » et possédant les informations suivantes.

- son numéro de passe « PASS ».
- son numéro d'identification « IDEN ».
- 25 - son numéro d'exemplaire « EXAM ».
- sa date de début de validité « DEVA ».
- sa date de fin de validité « FIVA ».
- son numéro de groupe horaire « GRHO ».
- sa liste de n numéro autorisations d'accès « AUAC ».
- 30 - ses caractères de contrôle « CACO ».

Sur la figure 2 on retrouve la centrale d'autorisation « CEAU » qui possède les informations suivantes.

- 35 - sa liste de n numéro de passe « PASS ».
- son fichier d'interdit « FIIN ».
- son mot d'encodage « MOEN ».
- son horloge « HORL ».
- sa liste de n numéro autorisations d'accès « AUAC ».
- 40 - sa liste de n tables d'horaires « TAHO ».

10

5 Avec les éléments selon l'invention des figures 1 et 2, pour qu'un processus puisse être lancé, il faut que les conditions suivantes soient remplies.

10 1°) Le caractère de contrôle « CACO » de la clef électronique « CLEL » de la figure 1 doit être valide pour que les lecteurs de clefs électroniques « LE-x » de la figure 2 transmettent le contenu des clefs électroniques « CLEL » de la figure 1 aux centrales d'autorisations « CEAU » de la figure 2.

15 2°) La centrale d'autorisation « CEAU » de la figure 2, après réception du contenu de la clef électronique « CLEL » de la figure 1, vérifie de nouveau le caractère de contrôle « CACO » de la clef électronique « CLEL » de la figure 1 qui doit être valide.

20 3°) Le mot d'encodage « MOEN » de la centrale d'autorisation « CEAU » de la figure 2 doit lui permettre de décoder les données de la clef électronique « CLEL » de la figure 1. Pour cela il faut que le mot d'encodage « MOEN » de la clef électronique « CLEL » de la figure 1 soit le même que celui de la centrale d'autorisation « CEAU » de la figure 2.

25 4°) Le numéro de passe « PASS » de la clef électronique « CLEL » de la figure 1 doit correspondre à l'un des n numéros de passe « PASS » de la centrale d'autorisation « CEAU » de la figure 2.

30 5°) Le numéro d'identification « IDEN » de la clef électronique « CLEL » de la figure 1 ne doit pas être présent dans la zone d'identification « IDEN » du fichier des interdits « FIIN » de la centrale d'autorisation « CEAU » de la figure 2. Si le numéro d'identification « IDEN » de la clef électronique « CLEL » de la figure 1 est présent dans la zone
35 d'identification « IDEN » du fichier des interdits « FIIN » de la centrale d'autorisation « CEAU » de la figure 2, le numéro d'exemplaire « EXAM » de la clef électronique « CLEL » de la figure 1 doit être supérieur au numéro d'exemplaire « EXAM » du fichier des interdits « FIIN » de la centrale d'autorisation
40 « CEAU » de la figure 2.

5 6°) La date de début de validité « DEVA » de la clef
électronique « CLEL » de la figure 1 doit être supérieure ou
égale à la date de l'horloge « HORL » de la centrale
d'autorisation « CEAU » de la figure 2 et la date de fin de
validité « FIVA » de la clef électronique « CLEL » de la figure
10 1 doit être inférieure ou égale à la date de l'horloge « HORL »
de la centrale d'autorisation « CEAU » de la figure 2.

7°) Le numéro du groupe horaire « GRHO » de la clef
électronique « CLEL » de la figure 1 doit faire référence à un
des numéros des tables d'horaires « TAHO » de la centrale
15 d'autorisation « CEAU » de la figure 2. Dans cette table
d'autorisation « TAHO » de la centrale d'autorisation « CEAU »
de la figure 2, il doit y avoir, pour le jour de la semaine
correspondant à celui de l'horloge « HORL » de la centrale
d'autorisation « CEAU » de la figure 2 une des n tranches de ce
20 jour donnant des heures valides. Pour être valide on doit avoir
l'heure de début de validité de la tranche supérieure ou égale à
l'heure de l'horloge « HORL » de la centrale d'autorisation
« CEAU » de la figure 2 et l'heure de fin de validité inférieure
ou égale à l'heure de l'horloge « HORL » de la centrale
25 d'autorisation « CEAU » de la figure 2.

8°) Le lecteur de clefs électroniques « LE-x » ($1 \leq x \leq n$)
de la figure 2, par lequel la demande de lancement de processus
a été effectuée, est lié au niveau de la centrale d'autorisation
« CEAU » de la figure 2 au processus « PR-x » ($1 \leq x \leq n$) de
30 la figure 2 par un numéro d'autorisation d'accès $1 \leq x \leq n$. Ce
numéro doit correspondre à l'un des n numéros d'autorisations
d'accès « AUAC » de la clef électronique « CLEL » de la figure
1.

35 Dans la figure 3, la clef électronique « CLEL » ne possède
pas de numéro de groupe horaire « GRHO » comme c'est le cas dans
la clef électronique « CLEL » de la figure 1 mais une table
d'horaire « TAHO ». Sur la figure 3, la clef électronique
« CLEL » encodée par le mot d'encodage « MOEN » possède donc les
40 informations suivantes.

12

- 5 - son numéro de passe « PASS ».
- son numéro d'identification « IDEN ».
- son numéro d'exemplaire « EXAM ».
- sa date de début de validité « DEVA ».
- sa date de fin de validité « FIVA ».
- 10 - sa table d'horaire « TAHO ».
- sa liste de n numéro autorisations d'accès « AUAC ».
- ses caractères de contrôle « CACO ».

15 Dans la figure 4, la centrale d'autorisation « CEAU » ne possède pas de tables d'horaires « TAHO » comme c'est le cas dans la centrale d'autorisation « CEAU » de la figure 2. Sur la figure 4 la centrale d'autorisation « CEAU » possède donc les informations suivantes.

- 20 - sa liste de n numéro de passe « PASS ».
- son fichier d'interdit « FIIN ».
- son mot d'encodage « MOEN ».
- son horloge « HORL ».
- sa liste de n numéro autorisations d'accès « AUAC ».

25

 Avec les éléments selon l'invention des figures 3 et 4, pour qu'un processus puisse être lancé, on retrouve les mêmes conditions que les éléments selon l'invention des figures 1 et 2 avec une différence sur la condition 7°) qui devient la

30 condition suivante.

 7°) Dans la table d'autorisation « TAHO » de la clef électronique « CLEL » de la figure 3, il doit y avoir, pour le jour de la semaine correspondant à celui de l'horloge « HORL »

35 de la centrale d'autorisation « CEAU » de la figure 4, une des n tranches de ce jour donnant des heures valides. Pour être valide on doit avoir l'heure de début de validité de la tranche supérieure ou égale à l'heure de l'horloge « HORL » de la centrale d'autorisation « CEAU » de la figure 3 et l'heure de

40 fin de validité inférieure ou égale à l'heure de l'horloge « HORL » de la centrale d'autorisation « CEAU » de la figure 3.

13

5

Les éléments selon l'invention, avec la structure des figures 1 et 2, des figures 5 et 6 donnent un exemple d'application particulière de l'invention.

10 La figure 5 représente un site sous la responsabilité d'un gestionnaire « G-1 ».

La centrale d'autorisation « CEAU-1 » de la figure 5 possède les informations suivantes.

15

- sa liste de 2 numéros de passe « PASS ».
- son fichier d'interdit « FIIN ».
- son mot d'encodage « MOEN-1 ».
- son horloge « HORL ».

20

- sa liste de 2 numéros autorisations d'accès « AUAC ».
- sa liste de 2 tables d'horaires « TAHO ».

La centrale d'autorisation « CEAU-2 » de la figure 5 possède les informations suivantes.

25

- sa liste de 1 numéro de passe « PASS ».
- son fichier d'interdit « FIIN ».
- son mot d'encodage « MOEN-1 ».
- son horloge « HORL ».

30

- sa liste de 1 numéro autorisations d'accès « AUAC ».
- sa liste de 1 table d'horaires « TAHO ».

La clef électronique « CLEL-1 » de la figure 5 encodée par le mot d'encodage « MOEN-1 » possède les informations suivantes.

35

- son numéro de passe « PASS ».
- son numéro d'identification « IDEN ».
- son numéro d'exemplaire « EXAM ».
- sa date de début de validité « DEVA ».
- sa date de fin de validité « FIVA ».
- son numéro de groupe horaire « GRHO ».

40

14

14

- 5 - sa liste de 1 numéro autorisation d'accès « AUAC ».
 - ses caractères de contrôle « CACO ».

 La clef électronique « CLEL-2 » de la figure 5 encodée par le mot d'encodage « MOEN-1 » possède les informations suivantes.

10

- son numéro de passe « PASS ».
 - son numéro d'identification « IDEN ».
 - son numéro d'exemplaire « EXAM ».
 - sa date de début de validité « DEVA ».

15

- sa date de fin de validité « FIVA ».
 - son numéro de groupe horaire « GRHO ».
 - sa liste de 2 numéros autorisations d'accès « AUAC ».
 - ses caractères de contrôle « CACO ».

- 20 La figure 6 représente un site sous la responsabilité d'un gestionnaire « G-2 ».

 La centrale d'autorisation « CEAU-1 » de la figure 6 possède les informations suivantes.

25

- sa liste de 1 numéro de passe « PASS ».
 - son fichier d'interdit « FIIN ».
 - son mot d'encodage « MOEN-2 ».
 - son horloge « HORL ».

30

- sa liste de 3 numéros autorisations d'accès « AUAC ».
 - sa liste de 1 table d'horaires « TAHO ».

 La clef électronique « CLEL-1 » de la figure 6 encodée par le mot d'encodage « MOEN-1 » possède les informations suivantes.

35

- son numéro de passe « PASS ».
 - son numéro d'identification « IDEN ».
 - son numéro d'exemplaire « EXAM ».
 - sa date de début de validité « DEVA ».

40

- sa date de fin de validité « FIVA ».
 - son numéro de groupe horaire « GRHO ».

15

- 5 - sa liste de 3 numéros autorisations d'accès « AUAC ».
 - ses caractères de contrôle « CACO ».

 Les lecteurs électroniques « LE-x » des figures 5 et 6 sont capables de vérifier les caractères de contrôle « CACO » des
10 clefs électroniques « CLEL-x » des figures 5 et 6. Les caractères de contrôle étant vérifiés, le contenu des clefs électroniques est envoyé aux centrales d'autorisations. A ce niveau, les lecteurs électroniques « LE-x » des figures 5 et 6 ne font pas de différences entre le gestionnaire « G-1 » de la
15 figure 5 et le gestionnaire « G-2 » de la figure 6.

 Les centrales d'autorisations « CEAU-x » des figures 5 et 6, après réception du contenu des clefs électroniques « CLEL-x » de la figure 5 et 6, vérifient de nouveau le caractère de contrôle « CACO » des clefs électroniques « CLEL-x » de la figure 5 et 6,
20 qui doit être valide. A ce niveau, les centrales d'autorisations « CEAU-x » des figures 5 et 6 ne font pas de différence entre le gestionnaire « G-1 » de la figure 5 et le gestionnaire « G-2 » de la figure 6.

 Les centrales d'autorisations « CEAU-x » de la figure 5 qui
25 possèdent le mot d'encodage « MOEN-1 » ne savent décoder que les clefs électroniques « CLEL-x » de la figure 5 qui sont encodées avec le même mot d'encodage « MOEN-1 ». De même les centrales d'autorisations « CEAU-x » de la figure 6 qui possèdent le mot d'encodage « MOEN-2 » ne savent décoder que les clefs
30 électroniques « CLEL-x » de la figure 5 qui sont encodées avec le même mot d'encodage « MOEN-2 ». L'utilisation du mot d'encodage dans le système permet aux centrales d'autorisations « CEAU-x » des figures 5 et 6 de faire la différence entre le gestionnaire « G-1 » de la figure 5 qui utilise le mot
35 d'encodage « MOEN-1 » et le gestionnaire « G-2 » de la figure 6 qui utilise le mot d'encodage « MOEN-2 ».

 La clef électronique « CLEL-1 » de la figure 5 qui possède le numéro de passe « PASS 225 » est reconnue par la centrale d'autorisation « CEAU-1 » de la figure 5 qui possède le même
40 numéro de passe « PASS 225 » mais pas par la centrale d'autorisation « CEAU-2 » de la figure 5 qui ne possède pas le

16

5 numéro de passe « PASS 225 ». La clef électronique « CLEL-2 » de
la figure 5 qui possède le numéro de passe « PASS 245 » est
reconnue par la centrale d'autorisation « CEAU-1 » et par la
centrale d'autorisation « CEAU-2 » de la figure 5 qui possèdent
le numéro de passe « PASS 245 ». La clef électronique « CLEL-1 »
10 de la figure 6 qui possède le numéro de passe « PASS 842 » est
reconnue par la centrale d'autorisation « CEAU-1 » de la figure
6 qui possède le même numéro de passe « PASS 842 ».
L'utilisation du numéro de passe dans le système permet de
limiter certaines clefs électroniques à certaines centrales
15 d'autorisations.

Le numéro d'identification « IDEN 185 » et d'exemplaire
« EXAM 4 » présent dans le fichier des interdits « FIIN » des
centrales d'autorisations « CEAU-1 et CEAU-2 » de la figure 5
interdit le lancement de processus par toutes les clefs
20 électroniques perdues ou volées ayant le numéro d'identification
« IDEN 185 » et un numéro d'exemplaire « EXAM compris de 1 à
4 ». De même le numéro d'identification « IDEN 120 » et
d'exemplaire « EXAM 1 » présent dans le fichier des interdits
« FIIN » des centrales d'autorisations « CEAU-1 » de la figure 6
25 interdit le lancement de processus par la clef électronique
perdue ou volée ayant le numéro d'identification « IDEN 120 » et
le numéro d'exemplaire « EXAM 1 ». L'utilisation du numéro
d'identification et du numéro d'exemplaire permet d'avoir un
fichier d'interdit mis à jour automatiquement par les centrales
30 d'autorisations selon la méthode expliquée dans la description
générale de l'invention.

Les dates de début et de fin de validité « DEVA » et
« FIVA » des clefs électroniques « CLEL-x » des figures 5 et 6
définissent la période pendant laquelle ces clefs électroniques
35 ont droit au lancement de processus. L'utilisation des dates de
validité permet de limiter au niveau mensuel et annuel les clefs
électroniques.

Les horaires qui définissent sur une semaine le droit au
lancement de processus de la clef électronique « CLEL-1 » de la
40 figure 5 ayant le groupe horaire « GRHO 2 » sont donnés par la
table d'horaires « TAHO 2 » de la centrale d'autorisation

17

5 « CEAU-1 » de la figure 5. Les horaires qui définissent sur une
semaine le droit au lancement de processus de la clef
électronique « CLEL-2 » de la figure 5 ayant le groupe horaire
« GRHO 1 » sont donnés par la table d'horaires « TAHO 1 » des
centrales d'autorisations « CEAU-1 et CEAU-2 » de la figure 5.
10 Les horaires qui définissent sur une semaine le droit au
lancement de processus de la clef électronique « CLEL-1 » de la
figure 6 ayant le groupe horaire « GRHO 1 » sont donnés par la
table d'horaires « TAHO 1 » de la centrale d'autorisation
« CEAU-1 » de la figure 6. L'utilisation des tables d'horaires
15 permet de limiter au niveau horaire et hebdomadaire les clefs
électroniques.

La clef électronique « CLEL-1 » de la figure 5 dont les
autorisations d'accès sont « AUAC 2 », peut lancer le processus
« PR-2 » de la centrale d'autorisation « CEAU-1 » de la figure
20 5. La clef électronique « CLEL-2 » de la figure 5 dont les
autorisations d'accès sont « AUAC 1 et 3 », peut lancer le
processus « PR-1 » de la centrale d'autorisation « CEAU-1 » de
la figure 5 et le processus « PR-3 » de la centrale
d'autorisation « CEAU-2 » de la figure 5. La clef électronique
25 « CLEL-1 » de la figure 6 dont les autorisations d'accès sont
« AUAC 1, 2 et 3 », peut lancer les processus « PR-1, PR-2 et
PR-3 » de la centrale d'autorisation « CEAU-1 » de la figure 6.
L'utilisation d'autorisation permet de limiter les processus
pouvant être lancé par une clef électronique.

REVENDEICATIONS

5

1. Système de contrôle de lancement de processus caractérisé en ce qu'il comporte une gestion des clefs électroniques basée sur la gestion d'un fichier des clefs électroniques interdites.

10

2. Système de contrôle de lancement de processus selon la revendication 1 caractérisé en ce que les clefs électroniques, pour permettre une gestion basée sur un fichier des interdits, comportent toutes les informations nécessaires à l'autorisation du lancement du processus.

15

3. Système de contrôle de lancement de processus selon les revendications 1 et 2 caractérisé en ce que les clefs électroniques sont encodées à l'aide d'un mot d'encodage « MOEN » pour permettre une différenciation du patrimoine des gestionnaires.

20

4. Système de contrôle de lancement de processus selon les revendications 1 à 3 caractérisé en ce que les centrales d'autorisations possèdent un moyen de décodage « MOEN » pour permettre le décodage des clefs électroniques encodées et la différenciation du patrimoine des gestionnaires.

25

5. Système de contrôle de lancement de processus selon les revendications 1 et 2 caractérisé en ce que les clefs électroniques possèdent un moyen « PASS » pour permettre une sélection des processus autorisés au niveau des centrales d'autorisations.

30

6. Système de contrôle de lancement de processus selon les revendications 1, 2 et 5 caractérisé en ce que les centrales d'autorisations possèdent des moyens « PASS » pour permettre une sélection des clefs électroniques et autoriser la clef électronique à lancer des processus au niveau des centrales d'autorisations.

35

40

19

5 7. Système de contrôle de lancement de processus selon les revendications 1 et 2 caractérisé en ce que les clefs électroniques comportent un moyen « IDEN » permettant d'identifier les clefs électroniques interdites.

10 8. Système de contrôle de lancement de processus selon les revendications 1, 2 et 7 caractérisé en ce que les clefs électroniques comportent un moyen « EXAM » permettant de déterminer l'exemplaire de la clef électronique.

15 9. Système de contrôle de lancement de processus selon les revendications 1, 2, 7 et 8 caractérisé en ce que les centrales d'autorisations comportent dans le fichier des interdits « FIIN » d'un moyen « IDEN » permettant d'identifier les clefs électroniques interdites.

20 10. Système de contrôle de lancement de processus selon les revendications 1, 2, 7, 8 et 9 caractérisé en ce que les centrales d'autorisations comportent dans le fichier des interdits « FIIN » d'un moyen « EXAM » permettant de déterminer
25 l'exemplaire de la clef électronique.

11. Système de contrôle de lancement de processus selon les revendications 1, 2, 7, 8, 9 et 10 caractérisé en ce que les centrales d'autorisations utilisent les informations
30 d'identification « IDEN » et d'exemplaire « EXAM » des clefs électroniques pour effectuer une mise à jour automatique du fichier des clefs électroniques interdites.

12. Système de contrôle de lancement de processus selon les
35 revendications 1 et 2 caractérisé en ce que les clefs électroniques comportent une date de début de validité « DEVA » et une date de fin de validité « FIVA » permettant de limiter dans le temps les droits, des clefs électroniques, au lancement des processus.

40

20

5 13. Système de contrôle de lancement de processus selon les revendications 1, 2 et 12 caractérisé en ce que les centrales d'autorisation comportent une horloge « HORL » donnant la date courante pour limiter dans le temps les droits, des clefs électroniques, au lancement des processus.

10

14. Système de contrôle de lancement de processus selon les revendications 1 et 2 caractérisé en ce que les clefs électroniques comportent une table d'horaires « TAHO » permettant de limiter de façon hebdomadaire et à la minutes près
15 les droits, des clefs électroniques, au lancement des processus.

15. Système de contrôle de lancement de processus selon les revendications 1 et 2 caractérisé en ce que les clefs électroniques comportent un numéro de groupe horaire « GRHO »
20 permettant de limiter de façon hebdomadaire et à la minutes près les droits, des clefs électroniques, au lancement des processus.

16. Système de contrôle de lancement de processus selon les revendications 1, 2 et 15 caractérisé en ce que les centrales
25 d'autorisation utilisent l'information de groupe horaire « GRHO » des clefs électroniques pour sélectionner une des tables d'horaires « TAHO ».

17. Système de contrôle de lancement de processus selon les
30 revendications 1, 2, 15 et 16 caractérisé en ce que les centrales d'autorisation comportent des tables d'horaires « TAHO » permettant de limiter de façon hebdomadaire et à la minutes près les droits, des clefs électroniques, au lancement des processus.

35

18. Système de contrôle de lancement de processus selon les revendications 1, 2, 14, 15, 16, et 17 caractérisé en ce que les centrales d'autorisation comportent une horloge « HORL » donnant l'heure courante pour limiter de façon hebdomadaire et à la
40 minute près les droits, des clefs électroniques, au lancement des processus.

5

19. Système de contrôle de lancement de processus selon les revendications 1 et 2 caractérisé en ce que les clefs électroniques comportent une liste de numéros des autorisations d'accès « AUAC » pour sélectionner les processus auxquels ont
10 droit les clefs électroniques.

20. Système de contrôle de lancement de processus selon les revendications 1, 2 et 19 caractérisé en ce que les centrales d'autorisations comportent une liste des numéros des
15 autorisations d'accès « AUAC » pour associer les lecteurs de clef électroniques aux processus et sélectionner les processus auxquels ont droit les clefs électroniques.

21. Système de contrôle de lancement de processus
20 caractérisé en ce que les clefs électroniques ayant accès à des lecteurs de technologies « proches » (contacts, proximité, magnétique) et à des lecteurs de technologies « distante » (infrarouge, radiofréquence) comportent un moyen technique « proche » et un moyen technique « distant » pour transmettre
25 leur identification et les données qu'elles contiennent.

22. Système de contrôle de lancement de processus selon la revendication 1 caractérisé en ce que les lecteurs de clefs électroniques ayant une technologie « proche » de contacts, sont
30 réalisés par des moyens uniquement mécaniques.

23. Système de contrôle de lancement de processus selon la revendication 1 caractérisé en ce que les lecteurs de clefs électroniques, interface utilisateurs et les centrales
35 d'autorisations, centre de décision, sont des fonctions séparées.

24. Système de contrôle de lancement de processus selon la revendication 1 caractérisé en ce que les terminaux portables
40 possèdent un lecteur/programmeur de clefs électroniques.

22

- 5 25. Système de contrôle de lancement de processus selon les revendications 1 et 24 caractérisé en ce que les terminaux portables possèdent une liaison sans fil pour la communication avec les centrales d'autorisations.
- 10 26. Système de contrôle de lancement de processus selon les revendications 1, 24 et 25 caractérisé en ce que les terminaux portables ne possèdent pas les écrans et les informations de gestions des centrales d'autorisations.
- 15 27. Système de contrôle de lancement de processus selon les revendications 1, 24, 25 et 26 caractérisé en ce que les terminaux portables ne mémorisent pas le mot d'encodage des clefs électroniques.

1/4

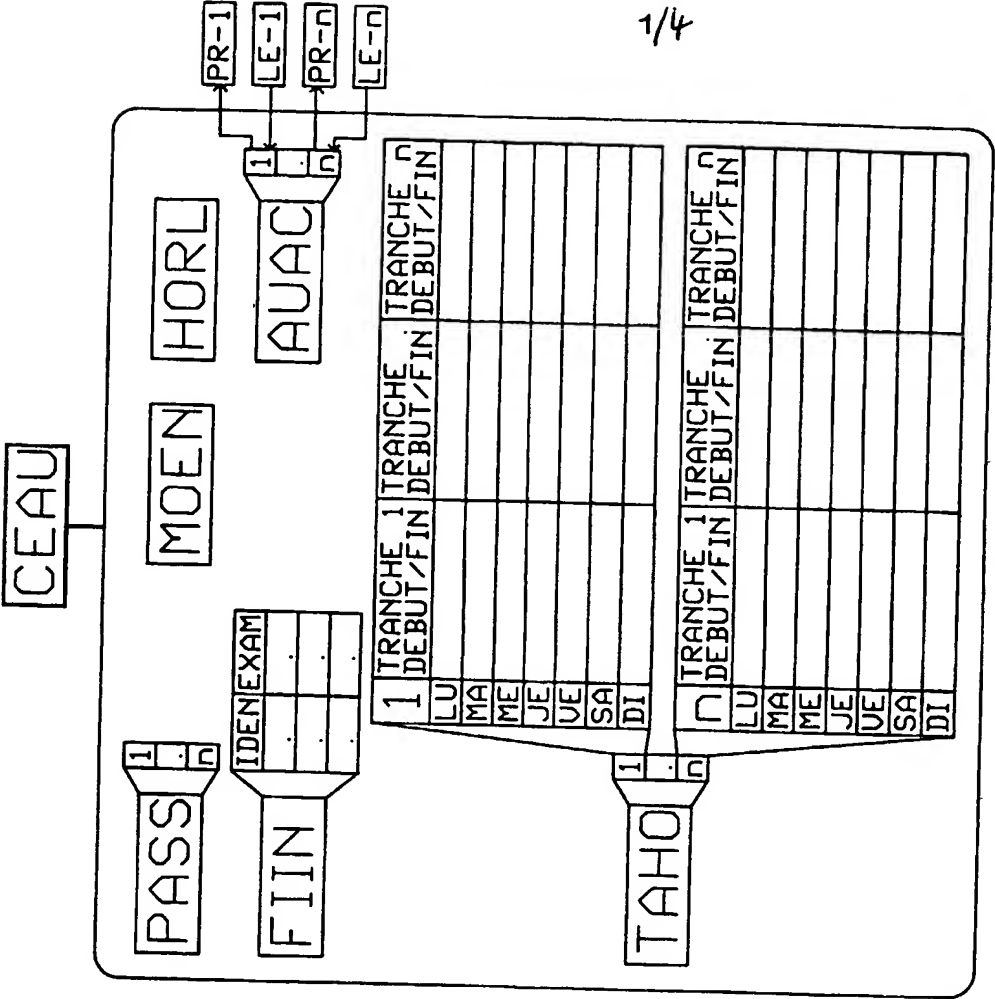


FIG. 2

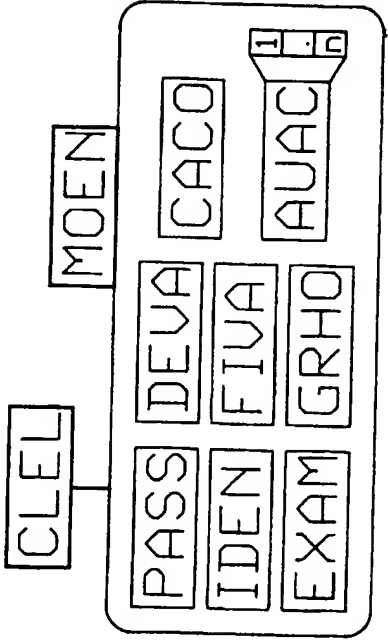
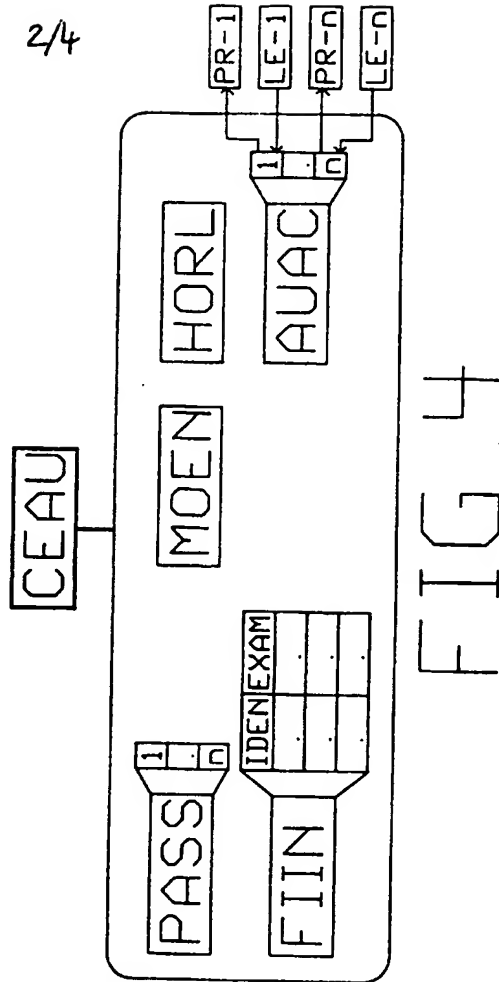
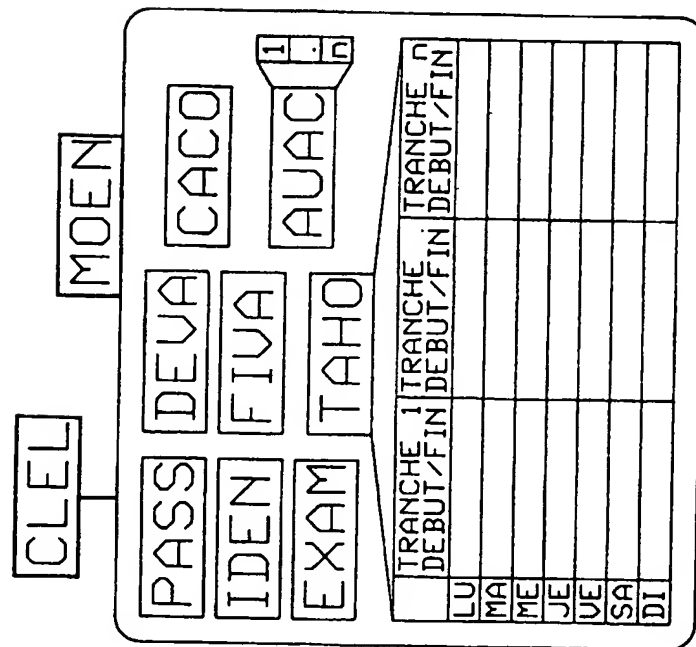


FIG. 1



3/4

G-1

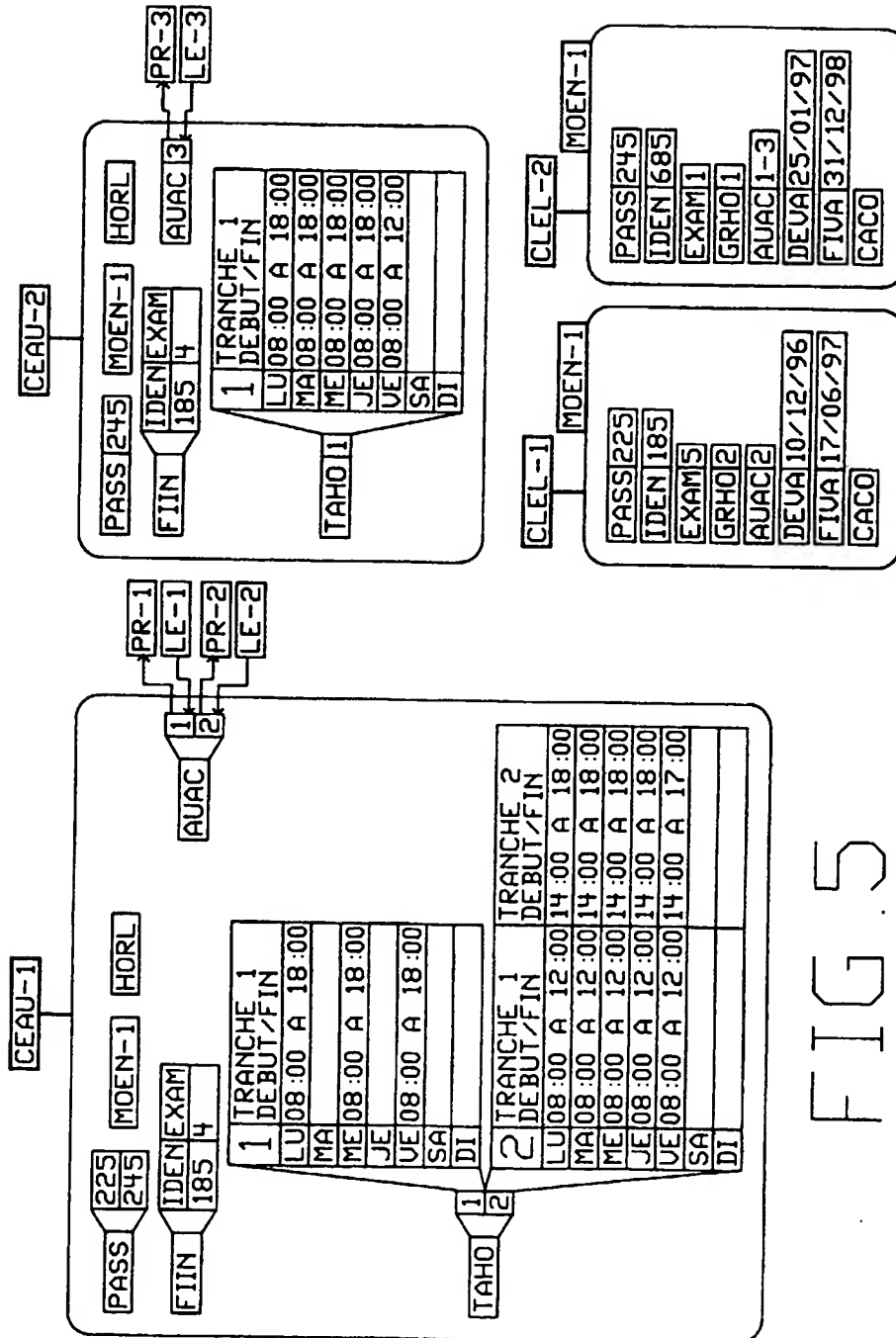


FIG 5

4/4

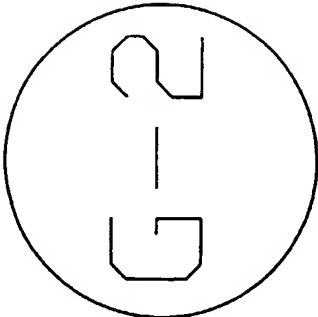
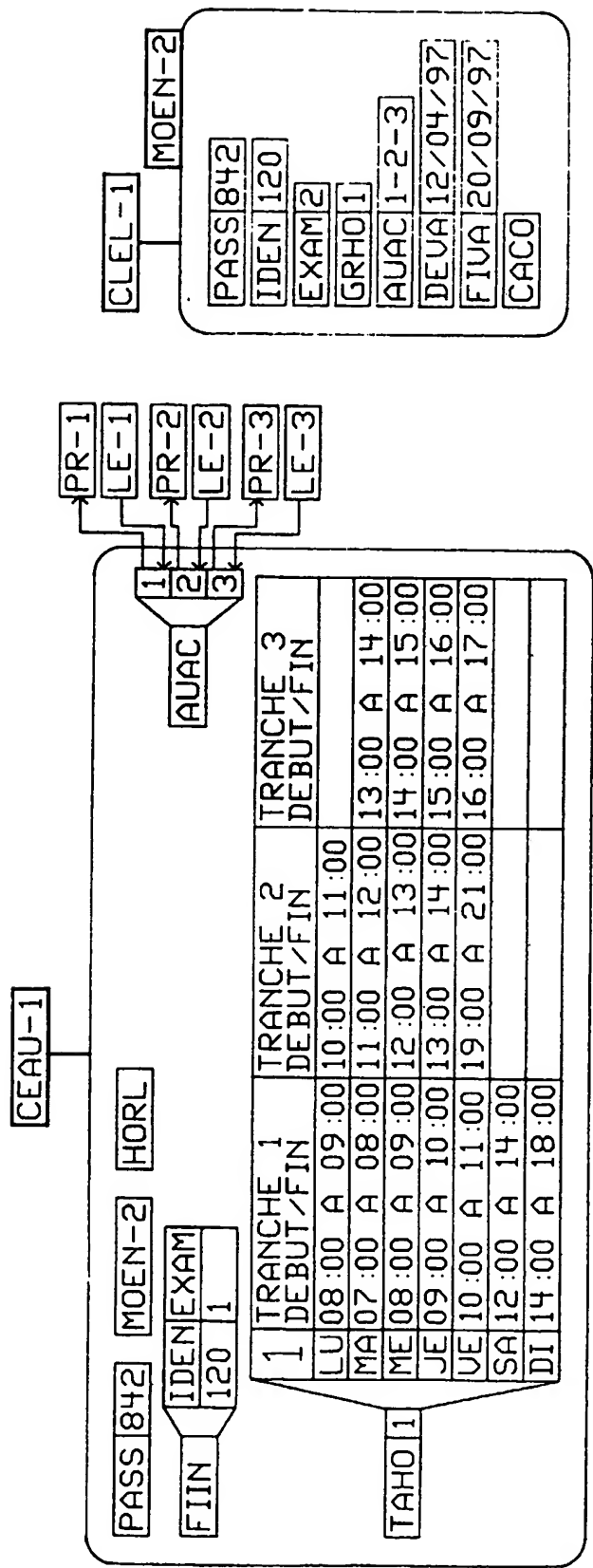


FIG 6